Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 14, NUMBER 1 >>> JANUARY 2014

Can the U.S. Congress Protect Vulnerable Targets from Cyber Thieves?

By Jason Crawford, Attorney, Washington, D.C.

The recent massive data breach at retail giant Target Corp. underscores the need for comprehensive cybersecurity legislation in the United States. In one of the largest retail cybercrimes in the nation's history, thieves made off with data from 40 million credit and debit card accounts of consumers, along with the personal information of at least 70 million customers, including names, e-mail addresses and telephone numbers. Experts estimate that, for large data breaches, the cost typically amounts to about $17 per account, which suggests that the breach could cost Target hundreds of millions of dollars.[1] Additionally, the company faces a nationwide probe from several state attorneys general, and members of the U.S. Congress have already called for hearings into the data theft.[2]

One upshot of the incident may be renewed attention from Congress on passing cybersecurity legislation. The attack prompted Sen. Patrick Leahy (D-Vt.), chairman of the Senate Judiciary Committee, to pledge to pursue cybersecurity legislation in 2014.[3]

Indeed, the ability of businesses to prevent cyber attacks will be hindered until Congress passes cybersecurity legislation that allows for information-sharing between companies and government agencies in order to fend off intrusions from the hackers, cyber thieves, and nation-states that target computer networks. Under the current legal regime, companies lack incentives to share cyber-threat information with the government for fear that sharing customers' information with the government will lead to privacy lawsuits.[4] This could change in 2014.

Previous Legislative Efforts Have Failed

Both companies and the government stand to benefit from the collection of data about the activities of hackers. Currently, a company may be aware of critical information about threats and vulnerabilities that would be useful for other companies to know, but the company may refrain from sharing information with authorities for fear of liability.

A 2012 study by the Homeland Security Project of the non-profit Bipartisan Policy Center (BPC) concluded that more public-private cyber information-sharing was needed to improve the detection of threats and to allow for coordinated responses to cyber attacks.[5] Information that should be shared includes malware threat signatures, malicious Internet protocol addresses, and immediate cyber attack incident details. The collection of this information would be limited to protecting against cybersecurity threats. The BPC recommended that Congress pre-empt certain state and federal laws in order to allow companies the freedom to share information with the government about cybersecurity incidents without fear of violating data breach and unfair trade practice laws.

2013 looked like a promising year for the passage of cybersecurity legislation. President Obama highlighted

the importance of cybersecurity legislation in his State of the Union address,[6] and a central feature of the White House's cybersecurity agenda is a plan to protect companies from privacy lawsuits when turning over data on electronic intrusions to the government.[7] Bipartisan support for a measure suggested that it was one of the few major legislative issues with the backing of both sides of the aisle in a divided Congress, and leaders of both parties signaled that a cybersecurity law was a top legislative priority in 2013.[8] But this was not to be.

The debate about cybersecurity legislation has often been framed as a matter of privacy versus security, and, in 2013, the privacy advocates prevailed. Leading public officials have pushed for improved cybersecurity and highlighted the nation's vulnerability to cyber attacks. Former Secretary of Defense Leon Panetta warned of a "cyber pearl harbor";[9] former Homeland Security Secretary Janet Napolitano spoke of a "cyber 9/11";[10] and former FBI Director Robert Mueller described cyber crimes as the "greatest threat to our country."[11] Yet these warnings have been drowned out by privacy concerns.

Companies insist that liability protection is needed to encourage real time information-sharing between the private and public sectors, but privacy advocates fear that too much data will end up in the hands of the government.

The proposed Cyber Intelligence Sharing and Protection Act (CISPA) was approved by a 288-127 vote in the House in April 2013, but it stalled in the Senate amid concerns from the White House that the bill did not require private entities to take reasonable steps to remove irrelevant personal information when sending cybersecurity data to the government or other private sector entities.[12] Privacy advocates also criticized the bill for lacking sufficient transparency about how information would be shared among government agencies.[13] Edward Snowden's revelations about the National Security Agency's (NSA) domestic surveillance program have made it even harder for cybersecurity legislation to gain momentum. Opponents of information-sharing now characterize such provisions as putting more information from U.S. citizens into the hands of the NSA.

Cybersecurity Legislation in 2014?

Congress's inability to pass cybersecurity legislation in 2013 does not mean that failure in 2014 is preordained. Several developments suggest that the passage of legislation is possible.

First, the business community is playing an increasingly active role in efforts to create a workable law. Earlier iterations of cybersecurity legislation, such as the proposed Cybersecurity Act of 2012, took a heavy regulatory approach that was opposed by many business leaders. The bill was defeated in part because of lobbying by the Chamber of Commerce, which argued that the measure would shift private sector resources away from implementing security measures and toward complying with government regulations.[14]

As newer drafts of bills have favored a voluntary approach, and as cyber threats have become a top concern of corporate leaders, perceptions about cybersecurity legislation among much of the business community appear to have shifted.

In September 2012, Sen. Jay Rockefeller (D-W.Va.), chairman of the Senate Commerce Committee, sent letters to all of the Fortune 500 chief executives asking about their cybersecurity practices and the federal government's role in developing those practices. According to a memorandum to Rockefeller from the Commerce Committee majority staff, approximately 300 companies responded to the letter, and the responses showed that much of the private sector was supportive of Congress's interest in passing cybersecurity legislation.[15] Notably, many executives stated that they supported provisions that would create a voluntary system for information-sharing between the private sector and the federal government.

In the past, business organizations actively lobbied against cybersecurity legislation, but now some trade groups are calling on Congress to pass legislation that would allow businesses and the government to share timely and actionable information on cyber threats. In November 2013, several financial industry trade groups wrote to the senior members of the Senate Select Committee on Intelligence saying that their ability to prevent cyber attacks was hindered by "a system that is weakened due to uncertainty over liability concerns."[16] In light of the recent breach at Target, it's likely that more members of the private sector will become active in shaping any cybersecurity bills coming out of Congress.

Furthermore, the executive branch will likely put pressure on Congress in 2014 to pass legislation that will supplement the executive order that President Obama signed in February 2013.Executive Order 13636 is aimed at creating new cybersecurity standards for the owners of critical infrastructure under the auspices of the National Institute for Standards and Technology (NIST).[17] NIST plans to release the official framework in February 2014. The standards are voluntary, and incentives — such as liability protection — are needed to entice companies to participate. Only Congress can create such incentives.

Section 4 of the executive order states that it is the government's policy "to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." While this creates a framework for the government to share information with the private sector, Congressional action is needed to encourage bi-directional information-sharing.

Practical Questions Remain

And many questions remain about what the information-sharing will look like in practice. The executive order envisions a voluntary system, but will the incentives be such that the private sector is forced to comply? Will companies retain their immunity if they act on government information that proves to be wrong? Finally, Congress will need to determine which agencies

   ISSN 1473-3579

will have access to the private sector information. Most likely, a civilian agency such as the Department of Homeland Security will take the lead, but some members of Congress have argued that the NSA should have access to the information.

In order for legislation to succeed in 2014, any proposed bills will need to address both privacy and security concerns by including mechanisms to protect privacy and civil liberties for any information that businesses share with the government.

It is possible that several previously stalled bills could return in a modified form in 2014 with more privacy protections. In October 2013, Sen. Dianne Feinstein (D-Calif.), chair of the Senate Select Committee on Intelligence, announced that she was working with Sen. Saxby Chambliss (R-Ga.) on a new version of CISPA that would address privacy concerns, while at the same time facilitating information-sharing by providing limited liability protections for companies that share information.[18] Previously, CISPA was criticized for giving companies blanket immunity for sharing broadly defined cyber "threat indicators" with the government. If a modified CISPA is to pass in 2014, it will need to include a narrowly tailored liability protection that will balance the need for consumer privacy against the need for information-sharing.

2014 may also see a vote on a Senate bill that was approved by the Commerce Committee but has since been relegated to the sidelines. In November 2013, Commerce Committee Chairman Rockefeller announced that he would submit the proposed Cybersecurity Act of 2013 as an amendment to the annual National Defense Authorization Act.[19] Rockefeller's maneuver gives the bill a much better chance of getting to the president's desk, but substantively the legislation is far less ambitious than earlier cybersecurity bills, including CISPA. The bill would codify President Obama's executive order regarding the cybersecurity framework of voluntary information technology security best practices being developed by NIST. However, the legislation would not grant companies liability protection in exchange for adopting NIST's voluntary cybersecurity guidelines or sharing information about online threats with each other and with the government.

Rockefeller's bill is a first step, but additional legislation will likely be needed to foster information-sharing between the government and industry.

A more robust system of public-private sharing would create better awareness about the nation's networks and allow both businesses and the government to make better decisions about how to defend them.

Until such legislation passes, there will be many more vulnerable Targets for cyber thieves.

NOTES

[1] David Henry and Karen Freifeld, *Target Breach Could Cost Hundreds of Millions, Probe Starts*, Reuters (Dec. 19, 2013), http://www.reuters.com/article/2013/12/20/target-breach-expenses-idUSL2N0JZ03I20131220.

[2] Dhanya Skariachan and Jim Finkle, *Target Breach Worse than Thought, States Launch Joint Probe*, Reuters (Jan. 11, 2014), http://in.reuters.com/article/2014/01/10/target-breach-idINDEEA090A620140110; Peter Schroeder, *Dems Call for Hearings in Wake of Target Data Theft*, The Hill (Dec. 30, 2013), http://thehill.com/blogs/on-the-money/banking-financial-institutions/194153-dems-call-for-hearings-in-wake-of-target.

[3] Press Release, Comment of Sen. Patrick Leahy (D-Vt.), Chairman, Senate Judiciary Committee, On Target Data Breach (Dec. 20, 2013), http://www.leahy.senate.gov/press/comment-of-senator-patrick-leahy-d-vt-chairman-senate-judiciary-committee-on-target-data-breach.

[4] *See, e.g.,* David Goldman, *President Obama Cracks Whip on Cybercrime*, CNN (Feb. 12, 2013), http://security.blogs.cnn.com/2013/02/12/president-obama-cracks-whip-on-cybercrime/?iref=allsearch.

[5] Bipartisan Policy Center's Homeland Security Project, *Cyber Security Task Force: Public-Private Information Sharing* (July 19, 2012), http://bipartisanpolicy.org/sites/default/files/Public-Private%20Information%20Sharing.pdf

[6] *See supra* note 4.

[7] *Cybersecurity Legislative Proposal*, Office of the President (May 12, 2011), http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[8] *See, e.g.,* Amber Corrin, *Election's End Revives Hope for Cybersecurity Action*, FCW (Nov. 8, 2012) http://fcw.com/articles/2012/11/08/cybersecurity-legilsation.aspx; Jennifer Martinez, *McCaul: Cybersecurity Legislation is 'Top' Priority Next Congress*, The Hill (Dec. 5, 2012), http://thehill.com/blogs/hillicon-valley/technology/271251-mccaul-cybersecurity-legislation-is-qtopq-priority-next-congress.

[9] Elisabeth Bumiller and Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. Times (Oct. 11, 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0.

[10] *U.S. Homeland Chief: Cyber 9/11 Could Happen "Imminently,"* Reuters (Jan. 24, 2013), http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.

[11] Stacy Cowley, *FBI Director: Cybercrime Will Eclipse Terrorism,* CNN (March 2, 2012), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/.

[12] Office of the President, *Statement of Administration Policy* (April 16, 2013), http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf.

[13] Robyn Greene, *CISPA's Problem Isn't Bad PR, It's Bad Privacy*, ACLU.org (March 28, 2013), https://www.aclu.org/blog/technology-and-liberty-national-security/cispas-problem-isnt-bad-pr-its-bad-privacy.

[14] R. Bruce Josten, *Key Vote Letter on S. 3414, the "Cybersecurity Act of 2012,"* USChamber.com (July 31, 2012), http://www.uschamber.com/issues/letters/2012/key-vote-letter-s-3414-cybersecurity-act-2012%E2%80%9D.

[15] Majority Staff, Senate Committee on Commerce, Science and Transportation, *Summary of the Feedback on Cybersecurity from "Fortune 500" Companies* (Jan. 28, 2013), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=5a85f211-a5c9-4306-9c84-d3a6b88024f6.

[16] Ryan Tracy, *Cybersecurity Legislation Gets Renewed Push from Financial Firms*, Wall St. J. (Nov. 13, 2013), http://blogs.wsj.com/washwire/2013/11/13/cybersecurity-legislation-gets-renewed-push-from-financial-firms/.

[17] Exec. Order No. 13636, 78 Fed. Reg. 11737 (Feb. 12, 2013).

[18] Dana Liebelson, *CISPA Zombie Bill Is Back, With Fewer Privacy Concerns . . . Maybe?*, Mother Jones (Oct. 21, 2013), http://www.motherjones.com/politics/2013/10/cispa-NSA-cybersecurity-feinstein-senate.

[19] Brendan Sasso, *Rockefeller to Offer Cybersecurity Amendment to Defense Bill*, The Hill (Nov. 21, 2013) http://thehill.com/blogs/hillicon-valley/191015-rockefeller-to-offer-cybersecurity-amendment-to-defense-bill.

Jason Crawford is a Law Clerk to Judge Thomas C. Wheeler on the United States Court of Federal Claims in Washington, D.C. The author wrote this article in his personal capacity. The opinions expressed are those of the author and do not necessarily reflect the views of his employer. The author may be contacted at jcrawford21@gmail.com.